entropy

Article

A Security Enhanced Encryption Scheme and Evaluation of Its Cryptographic Security

Miodrag J. Mihaljević

Mathematical Institute, The Serbian Academy of Sciences and Arts, 11000 Belgrade, Serbia;
miodragm@turing.mi.sanu.ac.rs

Received: 18 June 2019; Accepted: 15 July 2019; Published: 17 July 2019

Abstract: An approach for security enhancement of a class of encryption schemes is pointed out and its security is analyzed. The approach is based on certain results of coding and information theory regarding communication channels with erasures and deletion errors. In the security enhanced encryption scheme, the wiretapper faces a problem of cryptanalysis after a communication channel with bits deletion and a legitimate party faces a problem of decryption after a channel with bit erasures. This paper proposes the encryption-decryption paradigm for the security enhancement of lightweight block ciphers based on dedicated error-correction coding and a simulator of the deletion channel controlled by the secret key. The security enhancement is analyzed in terms of the related probabilities, equivocation, mutual information and channel capacity. The cryptographic evaluation of the enhanced encryption includes employment of certain recent results regarding the upper-bounds on the capacity of channels with deletion errors. It is shown that the probability of correct classification which determines the cryptographic security depends on the deletion channel capacity, i.e., the equivocation after this channel, and number of codewords in employed error-correction coding scheme. Consequently, assuming that the basic encryption scheme has certain security level, it is shown that the security enhancement factor is a function of the deletion rate and dimension of the vectors subject to error-correction encoding, i.e., dimension of the encryption block.

Keywords: encryption; cryptographic security enhancement; erasure error correction; channel with deletion errors; mutual information; channel capacity; the probability of classification error

1. Introduction

The main aim of the error-correction codes is overcoming the noise in public communication channels, but there is a long record of results on employment of error-correction coding theory for developing systems for secret communications. These systems belong to one of the following two main categories: the systems without the so called cryptographic keys, as well as the cryptographic keys controlled ones (see [1], for example).

The first coding based technique for secret communication over noisy channels without employment of cryptographic keys have been proposed in [2] where a dedicated coding scheme has been employed which provides secret communication over a public channel under assumption that the wiretapper faces sample collection through the channel with an ϵ higher noise in comparison with the one in the main channel over which communicate the legitimate parties, and a lot of papers have appeared as a follow-up of [2].

Employment of error-correction codes controlled by the cryptographic keys have been addressed in the both two major settings: the secret (symmetric) key setting and the public (asymmetric) key one. The most famous coding based system is McEliece public key encryption system [3] and this proposal has been followed by a number of results on its analysis and alternative proposals. McEleiece public key system is based on difficulty of decoding a random block error correcting code which is NP-complete in the worst case scenario as shown in [4].

Within the secret key cryptographic setting there are the following two major directions of employment error correction coding: (i) developing certain code-based encryption techniques; and (ii) enhancing security of certain lightweight encryption schemes. A number of symmetric key encryption schemes have been reported based on employment of the code-based and noisy channel paradigm. An illustrative and recent example on code-based secret key encryption schemes is the proposal [5] and its cryptanalysis reported in [6] which has shown insecurity of the proposal. The previous example illustrates that design of efficient code based symmetric encryption techniques appears as a tricky issue.

An alternative approach is to employ coding theory in symmetric key crypto-systems for security enhancement of certain lightweight encryption techniques, and goal of this paper is to add some novel results to this approach. Employment of results on error-correction coding and noisy channels for the security enhancement has been reported in a number of papers, and we could identify the following main directions within this approach. One direction is the enhancement employing a model of noisy channel with the additive noise and related coding results. The other direction is employment of the paradigm of the channels with synchronization errors and results on the related coding techniques. Illustrative techniques for security enhancement based on a model of noisy channels with additive errors have been reported in [7–11], and security evaluation of a generic model of these techniques from information-theoretic and computational complexity points of view are reported in [12,13], respectively. The enhancement approach based on the channels with synchronization errors and in particular an encryption approach which involves a communication channel with the errors in the form of *bits insertion* is reported in [14,15].

Motivation for the work. According to the above consideration of the topic, security enhancement of lightweight encryption techniques employing results on communication channels with synchronization errors and related coding appears as an interesting issue, and a particular goal could be consideration of the enhancement employing a deletion channel controlled by the secret key. Also, the addressed issue could be considered as a generalization of the shrinking and self-shrinking encryption techniques reported in [16,17], and a way to overcome the reported weaknesses of these techniques (see, [18–20], for example).

Summary of the results. This paper yields: (i) a proposal of the encryption-decryption scheme for the security enhancement of lightweight block ciphers based on a binary block error-correction coding and a simulator of the deletion channel controlled by the secret key, and (ii) cryptographic security evaluation of the proposed scheme. We suppose that a building component for developing security enhanced scheme is a block encryption algorithm with a known security level (specified by Definition 2), and we consider this algorithm which is the subject of enhancement as the "initial" encryption scheme. Main results of the paper are in Sections 2.2 and 4.2. Section 2.2 provides a construction for security enhancement of a given encryption scheme employing a suitable block error-correction code for a binary erasure channel which performs mapping $\{0,1\}^n \rightarrow \{0,1\}^{n'}$, $n' > n$, and a simulator of a binary channel with the deletions rate d controlled by the secret key. The construction is such that the wiretapper faces a problem of cryptanalysis after a communication channel with bits deletion and the legitimate party should only perform the decryption after a channel with bit erasures correctable by the employed error-correction code. The security enhancement is analyzed in terms of the related probabilities, equivocation, mutual information and channel capacity, and it includes employment of certain recent results regarding the upper-bounds on the capacity of channels with deletion errors. Main result of Section 4.2 is Theorem 1 which in a generic way proves the security enhancement showing that the adversary's probability to win the specified security evaluation game (specified by Definition 1) is reduced for certain factor $\delta << 1$ which upper bound is derived, and it is a decreasing function of the coding parameter n and the deletion rate d.

Organization. The paper is organized as follows. Section 2 proposes a framework for security enhancement based on the secret key controlled simulation of a deletion channel and dedicated error-correction coding. Technical background for the security evaluation is summarized in Section 3. Security evaluation results are given in Section 4, and the final Section 5 provides a concluding discussion.

2. A Proposal for the Security Enhanced Encryption

An encryption and decryption algorithm which provide a provably enhanced cryptographic security are proposed in this section. The enhanced security appears as a consequence of the design based on employment of the simulator of a binary noisy channel which appears as the erasure channel at the legitimate party and the deletion one at the wiretapper.

2.1. Underlying Ideas

The underlying ideas for the design could be summarized as follows. Enhance security of encryption based on information-theoretic and coding results when a wiretapper faces sample collection after a channel with deletions assuming a binary deletion channel with deletion probability d which takes input binary string and deletes each bit independently with the probability d. A model of the deletion channel is illustrated in Figure 1.

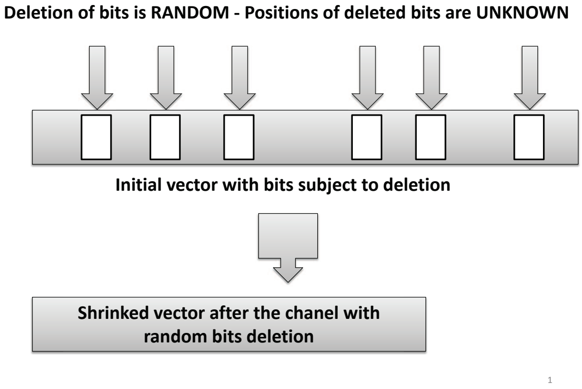
Deletion of bits is RANDOM - Positions of deleted bits are UNKNOWN
Initial vector with bits subject to deletion
Shrinked vector after the chanel with random bits deletion
1

Figure 1. A model of the deletion channel.

Let a string $\mathbf{Z} = \{0,1\}^n$ denotes an input to a binary deletion channel and let the deletion pattern $\mathcal{D}$ is an increasing subsequence of $\{1,2,\ldots,n\}$ representing the bits that are not deleted. Consequently, $\mathbf{Z}_{\mathcal{D}}$ denotes the "transformation" of $\mathbf{Z}$ after a deletion channel with deletion pattern $\mathcal{D}$.

Note that when the deletion pattern $\mathcal{D}$ is known, the deletion channel reduces to the erasure channel and we could consider that $(\mathcal{D}, \mathbf{Z}_{\mathcal{D}})$ is the output of erasure channel for given input $\mathbf{Z}$.

The main underlying idea which this paper employs is to enhance cryptographic security of a given encryption scheme in such a way that a legitimate user faces an erasure channel, and a wiretapper faces a deletion channel, i.e., a legitimate party knows the deletion pattern $\mathcal{D}$ and a wiretapper does not know this pattern. Assuming that the deleted bits positions are selected in a pseudorandom manner controlled by the secret key and generated by the encryption/decryption algorithm, note that the legitimate party knows $\mathcal{D}$, but the wiretapper who does not know the secret key does not know $\mathcal{D}$ and consequently faces a deletion channel instead the erasure one faced by a legitimate party. Accordingly, the corresponding paradigm is displayed in Figure 2.

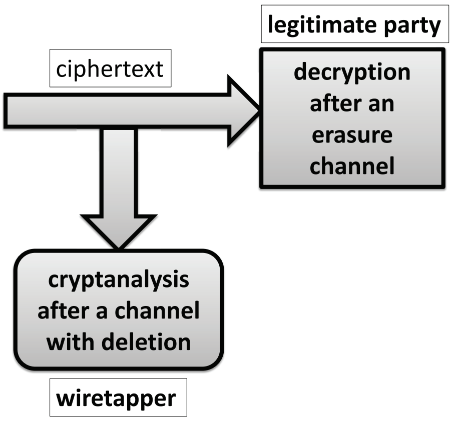
legitimate party
ciphertext
decryption after an erasure channel
cryptanalysis after a channel with deletion
wiretapper

Figure 2. Model of the decryption at a legitimate party versus cryptanalysis at the wiretapper side which faces problem of cryptanalysis after a channel with deletion errors.

2.2. Framework for Encryption and Decryption

The design proposed in this paper is based on the following building blocks:

- a lightweight block cipher;
- implementation of an error correction code encoding/decoding for binary erasure channel;
- simulation of a deletion channel where the deletion pattern $\mathcal{D}$ is generated by the employed block cipher.

It is assumed that encryption and decryption parties share a secret key. As usually, before the session, the both parties (encryption and decryption ones) establish a session key (to be used later on), employing the secret key and the public data.

The encryption and decryption are performed as follows.

- Encryption:
  - a lightweight block cipher generates n dimensional binary vector $\mathbf{C}' = E_{\mathbf{K}}(\mathbf{M})$ where $E_{\mathbf{K}}(\cdot)$ denotes the block cipher encryption according to the secret key $\mathbf{K}$ and performs one-to-one mapping $\{0,1\}^n \to \{0,1\}^n$;
  - an erasure error correction encoding capable to provide correction up to t erasure errors generates n''-bit vector $\mathbf{C}''$ as the corresponding mapping $\{0,1\}^n \to \{0,1\}^{n''}$, $n'' > n$, where t is a given parameter, and $n'' - t > n$;
  - a simulator of a binary channel with random bits deletion performs mapping $\{0,1\}^{n''} \to \mathbf{C} \in \{0,1\}^{n''-\ell}$ controlled by a vector $\mathbf{X}$ generated by the employed block cipher, $\ell \leq t$.
- Decryption:
  - an erasure error correction decoding controlled by a vector $\mathbf{X}$ generated by the employed block cipher generates n-bit vector $\mathbf{C}'$ by the corresponding mapping $\{0,1\}^{n''-\ell} \to \{0,1\}^n$, $\ell \leq t$;
  - a lightweight block cipher generates n dimensional binary vector $\mathbf{M} = E_{\mathbf{K}}^{-1}(\mathbf{C}')$ where $E_{\mathbf{K}}^{-1}(\cdot)$ denotes the block cipher decryption according to the secret key $\mathbf{K}$.

The proposed encryption and decryption framework is displayed in Figure 3.

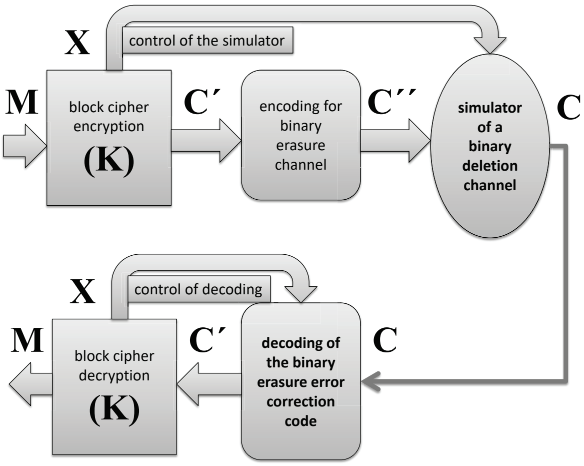
X
control of the simulator
M
block cipher encryption
(K)
C′
encoding for binary erasure channel
C′′
simulator of a binary deletion channel
C
X
control of decoding
M
block cipher decryption
(K)
C′
decoding of the binary erasure error correction code
C

Figure 3. Model of a security enhanced encryption employing a simulator of a noisy channel which appears as a deletion channel from the wiretappers prospective: the upper part shows the transmitter, and the lower part the receiver.

The objective of this paper is to provide a framework for the security enhancement and show the enhancement gain. Accordingly, consideration of particular instantiations of the framework is out of the scope of this paper. We just point out that a candidate coding scheme could be the polar coding, and that [21] provides an illustrative discussion of polar coding over a binary erasure channel, as well as the decoding complexity after a deletion channel.

Regarding similarity/dissimilarity of the proposed framework and the one reported in [5], note the following. The scheme [5] is based on a suitable block error-correction code and two shift registers which provide that the wiretapper faces a problem of decoding after a channel with flipping, insertion and deletion of the codeword bits. On the other hand, the proposed scheme is based on an (initial) encryption algorithm which has certain security level and a simulator of the deletion channel which in a provable way enhances security of the entire scheme. So, although the block representation of the both schemes has a similarity, they are substantially different because the one reported in [5] is a code-based design of encryption and the one proposed in this paper belongs to a class of the security enhanced encryption employing dedicated coding and simulator of a noisy channel.

3. Security Evaluation Background

3.1. Notations and Preliminaries

A random variable is denoted by an upper-case letter (e.g., A) and its realization is denoted by a lower-case letter (e.g., a). The entropy of a random object A is denoted by $H(A)$, and the mutual information between two random objects A and B is denoted by $I(A;B)$. The binary entropy function is denoted by $h(p) = -p\log_2 p - (1-p)\log_2(1-p)$.

The entropy of a random variable A is defined as:

$$H(A) := \sum_{x \in support(A)} Pr[A = a] \log_2 \frac{1}{Pr[A = a]}, \tag{1}$$

The mutual information $I(A;B)$ between jointly distributed random variables A and B is defined as follows:

$$I(A;B) := H(A) - H(A|B) = H(B) - H(B|A) \tag{2}$$

where conditional entropy is defined as

$$H(A|B) = \sum_{b \in supp(B)} Pr(B = b) H(A|B = b) \tag{3}$$

and

$$H(A|B = b) = \sum_{a \in supp(A)} Pr(A = a|B = b) \log_2 \frac{1}{Pr(A = a|B = b)} \tag{4}$$

Consequently, the conditional mutual information when the third variable Z is given is:

$$I(A, B|Z) := H(A|Z) - H(A|B, Z) = H(B|Z) - H(B|A, Z). \tag{5}$$

Following [1], the mutual information $I(\mathbf{M}; \mathbf{C})$ between the message $\mathbf{M}$ and the related sample $\mathbf{C}$, or the uncertainty, i.e., the equivocation $H(\mathbf{M}|\mathbf{C})$ are traditionally employed as the main information-theoretic security metric. On the other hand, according to certain recent considerations, the average mutual information $\bar{I}(\mathbf{M}, \mathbf{C})$ should be addressed as a strong information-theoretic security metric, and $\frac{1}{n}\bar{I}(\mathbf{M}, \mathbf{C})$ as a corresponding weak one.

3.2. The Probability of Error and The Equivocation after a Noisy Channel

Let A and B be discrete random variables which correspond to input and output, respectively, of a communication channel. Let the possible realizations of A and B are a_i, $i = 1, 2, \ldots, m$ and b_i, $i = 1, 2, \ldots, n$, respectively, $m > n$, and let a decision rule on A when B can be considered as identification of a realization a_i when b_i is given, and we denote by P_{err} the probability of the identification (classification) error.

Suppose the random variables A and B represent input and output messages (out of m possible messages), and the given conditional entropy $H(A|B)$ represents the average amount of information lost on A when B is given. According to [22] or [23], for example, we have the following general upper bound on the equivocation:

$$H(A|B) \leq h(P_{err}) + P_{err} \log_2(m - 1) \tag{6}$$

where $h(\cdot) \leq 1$ is the binary entropy function and $P_{err} = 1 - \Pr(A = a_i|B = b_i)$. The above inequality can be rewritten as follows:

$$H(A) - I(A, B) \leq h(P_{err}) + P_{err} \log_2(m - 1), \tag{7}$$

and when A is such that it has the maximum possible entropy we have:

$$m - I(A, B) \leq h(P_{err}) + P_{err} \log_2(m - 1), \tag{8}$$

which can be further transformed into:

$$1 - \frac{I(A, B)}{m} \leq \frac{1}{m} + \frac{P_{err}}{m} \log_2(m - 1). \tag{9}$$

3.3. The Capacity of a Deletion Channel

The Shannon capacity of a channel is denoted by Cap and is defined as

$$Cap := sup\{I(A; B)\}, \tag{10}$$

where A corresponds the channel input, B corresponds to the channel output, and the supremum is over the choice of the distribution of A.

As reported in [24], the capacity $Cap(d)$ of a deletion channel with the deletion rate d is upperbounded as follows:

$$Cap(d) = (1-d)log_e \frac{1+\sqrt{5}}{2} \tag{11}$$

for $d > 1/2$, and logarithm is taken to base e.

4. Security Evaluation of the Enhanced Encryption

4.1. Security Notation

We employ a traditional approach for analyzing cryptographic security based on the following two issues: (i) a description of what a "break" of the scheme means, and (ii) a specification of the assumed power of the adversary. A cryptographic scheme is considered as secure one in a computational sense, if for every probabilistic polynomial-time adversary $\mathcal{A}$ performing an attack of some specified type, and for every polynomial $p(n)$, there exists an integer N such that the probability that $\mathcal{A}$ succeeds (where success of the attack is also well-defined) is less than $\frac{1}{p(n)}$ for every $n > N$. Accordingly, the following two definitions specify a security evaluation scenario and a security statement.

Definition 1. *The Adversarial Indistinguishability Experiment consists of the following steps:*

1. *The adversary $\mathcal{A}$ chooses a pair of messages $(\mathbf{m}_0; \mathbf{m}_1)$ of the same length n, and passes them on to the encryption system for encrypting.*
2. *A bit $b \in \{0,1\}$ is chosen uniformly at random, and only one of the two messages $(\mathbf{m}_0; \mathbf{m}_1)$, precisely $\mathbf{m}_b$, is encrypted into ciphertext $\mathrm{Enc}(\mathbf{m}_b)$ and returned to $\mathcal{A}$;*
3. *Upon observing $\mathrm{Enc}(\mathbf{m}_b)$, and without knowledge of b, the adversary $\mathcal{A}$ outputs a bit b_0;*
4. *The experiment output is defined to be 1 if $b_0 = b$, and 0 otherwise; if the experiment output is 1, denoted shortly as the event $(\mathcal{A} \rightarrow 1)$, we say that $\mathcal{A}$ has succeeded.*

Definition 2. *An encryption scheme provides indistinguishable encryptions in the presence of an eavesdropper, if for all probabilistic polynomial-time adversaries $\mathcal{A}$*

$$\Pr[\mathcal{A} \rightarrow 1 | \mathrm{Enc}(\mathbf{m}_b)] \leq \frac{1}{2} + \epsilon \; , \tag{12}$$

where $\epsilon = \mathrm{negl}(n)$ is a negligibly small function.

Definitions 1 and 2 are more precisely discussed in [25].

4.2. Evaluation of the Security Gain

We consider the encryption/decryption scheme proposed in Section 2.2 which is a security enhanced scheme of certain basic one. Our goal is to estimate the advantage of $\mathcal{A}$ in the indistinguishability game specified by Definition 1 when $\mathbf{c} \leftarrow \mathrm{Enc}(\mathbf{m}_b)$ where $\mathbf{c}$ is a particular realization of $\mathbf{C}$, assuming that the advantage of $\mathcal{A}$ is known when $\mathbf{m}_0$ and $\mathbf{m}_1$ are two chosen realizations of $\mathbf{M}$ and the corresponding realization $\mathbf{c}'_b$ of $\mathbf{C}'$ is given, i.e., the advantage of $\mathcal{A}$ is known for the basic (security non-enhanced) scheme.

We assume that in the corresponding statistical model, the considered encryption scheme is such that

$$I(\mathbf{X}, \mathbf{C}) = 0 \quad \text{and} \quad I(\mathbf{X}, \mathbf{C} | \mathbf{M}) = 0 \; , \tag{13}$$

i.e., the knowledge of $\mathbf{C}$ and $\mathbf{M}$ does not leak (provide) any information on $\mathbf{X}$.

Lemma 1. *Let the mapping of* $\mathbf{m}$ *into* $\mathbf{c}'$ *be such that* $\frac{1}{2}+\epsilon$ *equals the advantage of the adversary* $\mathcal{A}$ *(specified by Definition 2) to win the indistinguishability game (specified by Definition 1). Under these assumptions,*

$$\Pr[\mathcal{A} \to 1|\mathbf{C} = \mathbf{c}] = \frac{1}{2} + \epsilon \cdot \delta$$

where

$$\delta \overset{\Delta}{=} \Pr(\mathbf{C}'' = \mathbf{c}''_b|\mathbf{C} = \mathbf{c}) \ . \tag{14}$$

Proof. For simplicity, it is assumed that $\frac{1}{2}+\epsilon$ equals the advantage of the adversary $\mathcal{A}$ (specified by Definition 2) to win the indistinguishability game. Consequently, let b which denotes the index of the selected message be realization of the random variable B.

The probability $\Pr(B = b|\mathbf{C} = \mathbf{c})$ that $\mathcal{A}$ wins the game is determined by the following.

$$\begin{aligned} \Pr(B = b|\mathbf{C} = \mathbf{c}) &= \frac{\Pr(B = b, \mathbf{C} = \mathbf{c})}{\Pr(\mathbf{C} = \mathbf{c})} \\ &= \frac{\sum_{\mathbf{x}} \Pr(B = b, \mathbf{C} = \mathbf{c}, \mathbf{C}'' = \mathbf{c}'')}{\Pr(\mathbf{C} = \mathbf{c})} \\ &= \frac{\sum_{\mathbf{x}} \Pr(B = b|\mathbf{C} = \mathbf{c}, \mathbf{C}'' = \mathbf{c}'')\Pr(\mathbf{C} = \mathbf{c}, \mathbf{C}'' = \mathbf{c}'')}{\Pr(\mathbf{C} = \mathbf{c})} \\ &= \frac{\sum_{\mathbf{c}''} \Pr(B = b|\mathbf{C}'' = \mathbf{c}'')\Pr(\mathbf{C} = \mathbf{c}, \mathbf{C}'' = \mathbf{c}'')}{\Pr(\mathbf{C} = \mathbf{c})} \ . \end{aligned} \tag{15}$$

The lemma assumption implies:

$$\Pr(B = b|\mathbf{C}' = \mathbf{c}'_b) = \frac{1}{2} + \epsilon \ , \tag{16}$$

where $\mathbf{c}'_b$ corresponds to the selected $\mathbf{m}_b$, and

$$\Pr(B = b|\mathbf{C}'' = \mathbf{c}'') = \frac{1}{2} \ \text{ for any } \mathbf{c}' \neq \mathbf{c}'_b \ . \tag{17}$$

Note that the encoding mapping $\mathbf{c}' \to \mathbf{c}''$ is a deterministic one-to-one mapping and consequently has no impact on the advantage of adversary $\mathcal{A}$, i.e., we have:

$$\Pr[\mathcal{A} \to 1|\mathbf{C}'' = \mathbf{c}''] = \Pr[\mathcal{A} \to 1|\mathbf{C}' = \mathbf{c}'] = \frac{1}{2} + \epsilon \ . \tag{18}$$

Consequently,

$$\Pr(B = b|\mathbf{C} = \mathbf{c}) =$$
$$\frac{\Pr(B = b|\mathbf{C}'' = \mathbf{c}''_b)\Pr(\mathbf{C} = \mathbf{c}, \mathbf{C}'' = \mathbf{c}''_b)}{\Pr(\mathbf{C} = \mathbf{c})} +$$
$$\frac{\sum_{\mathbf{c}'':\mathbf{c}'' \neq \mathbf{c}''_b} \Pr(B = b|\mathbf{C}'' = \mathbf{c}'')\Pr(\mathbf{C} = \mathbf{c}, \mathbf{C}'' = \mathbf{c}'')}{\Pr(\mathbf{C} = \mathbf{c})} \ ,$$

Finally, we obtain:

$$\Pr(B = b|\mathbf{C} = \mathbf{c}) =$$
$$\frac{(\frac{1}{2} + \epsilon)\Pr(\mathbf{C} = \mathbf{c}, \mathbf{C}'' = \mathbf{c}''_b) - \frac{1}{2}\Pr(\mathbf{C} = \mathbf{c}, \mathbf{C}'' = \mathbf{c}''_b)}{\Pr(\mathbf{C} = \mathbf{c})}$$
$$+ \frac{\frac{1}{2} \sum_{\mathbf{c}''} \Pr(\mathbf{C} = \mathbf{c}, \mathbf{C}'' = \mathbf{c}'')}{\Pr(\mathbf{C} = \mathbf{c})}$$

$$= \frac{1}{2} + \epsilon \cdot \Pr(\mathbf{C}'' = \mathbf{c}''_b | \mathbf{C} = \mathbf{c}) \; . \tag{19}$$

QED □

Definition 1 implies that the security of an encryption scheme increases as difference on the adversary $\mathcal{A}$ advantage from $\frac{1}{2}$ decreases: The factor $\delta < 1$ shows the reduction rate of the advantage, and so we call it the advantage reduction factor.

Theorem 1. *Let the basic encryption mapping $\{0,1\}^n \to \{0,1\}^n$ of $\mathbf{m}$ into $\mathbf{c}'$, be such that $\frac{1}{2}+\epsilon$ equals the advantage of the adversary $\mathcal{A}$ (specified by Definition 2) to win the indistinguishability game (specified by Definition 1), and the simulated deletion channel has the deletion rate d. Consequently, the advantage of the adversary $\mathcal{A}$, in the security enhanced scheme specified in Section 2.2 is:*

$$\Pr[\mathcal{A} \to 1 | \mathbf{C} = \mathbf{c}] < \frac{1}{2} + \epsilon \cdot \frac{(1-d)log_e\frac{1+\sqrt{5}}{2} + 1}{\log_2(2^n - 1)} \quad . \tag{20}$$

Proof. According to the (9) we have

$$1 - \frac{I(\mathbf{C}'', \mathbf{C})}{n} \leq \frac{1}{n} + \frac{P_{err}}{n} \log_2(2^n - 1) \; , \tag{21}$$

and taking into account that

$$P_{err} = 1 - \Pr(\mathbf{C}'' = \mathbf{c}''_b | \mathbf{C} = \mathbf{c}) \tag{22}$$

we obtain

$$\frac{1}{n}\Pr(\mathbf{C}'' = \mathbf{c}''_b | \mathbf{C} = \mathbf{c}) \log_2(2^n - 1) \leq -1 + \frac{I(\mathbf{C}'', \mathbf{C})}{n} + \frac{1}{n} + \frac{1}{n}\log_2(2^n - 1) < \frac{I(\mathbf{C}'', \mathbf{C})}{n} + \frac{1}{n} \; , \tag{23}$$

and

$$\Pr(\mathbf{C}'' = \mathbf{c}''_b | \mathbf{C} = \mathbf{c}) < \frac{I(\mathbf{C}'', \mathbf{C}) + 1}{\log_2(2^n - 1)} \; . \tag{24}$$

Finally, taking into account (10) and (11) we have:

$$\Pr(\mathbf{C}'' = \mathbf{c}''_b | \mathbf{C} = \mathbf{c}) < \frac{(1-d)log_e\frac{1+\sqrt{5}}{2} + 1}{\log_2(2^n - 1)} \; . \tag{25}$$

Substitution of (25) into the statement of Lemma 1 yields the proof. QED □

Lemma 1 shows that the encryption mapping $\mathbf{m} \rightarrow \mathbf{c}$ enhances the security because the probability that $\mathcal{A}$ wins the game becomes closer to $\frac{1}{2}$, which corresponds to random guessing, by the factor δ, and Theorem 1 shows that the upper bound on δ is $\frac{(1-d)log_e\frac{1+\sqrt{5}}{2}+1}{\log_2(2^n-1)} << 1$. Accordingly, Table 1 provides a numerical illustration on the upper bound on δ which determines reduction of the advantage of $\mathcal{A}$.

Table 1. A numerical illustration of the advantage reduction factor δ upper bound (which shows minimum reduction of the advantage of $\mathcal{A}$) as a function of the encryption scheme parameters d and n, the deletion rate and encryption block size, respectively.

d	Upper Bound on δ for $n = 64$	Upper Bound on δ for $n = 128$
0.55	0.01901	0.00950
0.60	0.01863	0.00931
0.65	0.01825	0.00912
0.70	0.01788	0.00894
0.75	0.01750	0.00875
0.80	0.01712	0.00856
0.85	0.01675	0.00837
0.90	0.01637	0.00819
0.95	0.01600	0.00800
0.99	0.01570	0.00785

5. Concluding Notes

This paper has proposed a framework for security enhancement of certain encryption schemes and its security evaluation. The final security evaluation result given in Theorem 1 also shows the security gain which the security enhanced encryption provides in comparison with the initial one. The lower bound on the security gain is a function of the encryption block size and the deletion rate in the simulated channel with deletion errors. The result given in Theorem 1 is a generic one and it holds for any particular instantiation of the proposed encryption framework.

An interesting future direction is design of particular instantiations of the proposed framework within the given implementation constraints where dedicated basic (initial) encryption, a code for correction of erasure errors and simulator of a channel with deletion errors controlled by the secret key are specified, and complexity of implementation overhead implied by the enhancement is evaluated. Regarding overhead implied by employment of the coding scheme, as an illustration, we point to the polar coding [21] which provides encoding and decoding complexities $O(n'' \log_2 n'')$ assuming that the encoding performs the mapping $\{0,1\}^n \to \{0,1\}^{n''}$, $n'' > n$.

Funding: This research was funded by the Ministry of Education, Science and Technological Development of Republic Serbia, project ON174008.

Acknowledgments: The Author thanks to the Anonymous Reviewers for the comments and suggestions resulting in improvement of the presentation.

Conflicts of Interest: The author declares no conflicts of interest.

References

1. Shannon, C.E. Communication theory of secrecy systems. *Bell Syst. Tech. J.* **1949**, *28*, 656–715. [CrossRef]
2. Wyner, A.D. The wire-tap channel. *Bell System Tech. J.* **1975**, *54*, 1355–1387. [CrossRef]
3. McEliece, R.J. A public-key cryptosystem based on algebraic coding theory. In *Deep Space Network*; Progress Report 42-44; Jet Propulsion Laboratory, California Institute of Technology: Pasadena, CA, USA, 1978; pp. 114–116.
4. Berlekamp, E.; McEliece, R.; van Tilborg, H. On the inherent intractability of certaincoding problems. *IEEE Trans. Inf. Theory* **1978**, *24*, 384–386. [CrossRef]
5. Esmaeili, M.; Gulliver, T.A. A secure code based cryptosystem via random insertions, deletions, and errors. *IEEE Commun. Lett.* **2016**, *20*, 870–873. [CrossRef]
6. Lee, Y.; Kim, Y.S.; No, J.S. Ciphertext-only attack on linear feedback shift register-based Esmaeili-Gulliver cryptosystem. *IEEE Commun. Lett.* **2017**, *21*, 971–974. [CrossRef]
7. Gilbert, H.; Robshaw, M.J.B.; Seurin, Y. How to encrypt with the LPN problem. (ICALP 2008). *Lect. Notes Comput. Sci.* **2008**, *5126*, 679–690.

8. Mihaljević, M.J.; Imai, H. An approach for stream ciphers design based on joint computing over random and secret data. *Computing* **2009**, *85*, 153–168. [CrossRef]
9. Mihaljević, M.J. A framework for stream ciphers based on pseudorandomness, randomness and error-correcting coding. In *Enhancing Cryptographic Primitives with Techniques from Error Correcting Codes*; Preneel, B., Dodunekov, S., Rijmen, V., Nikova, S., Eds.; IOS Press: Amsterdam, The Netherlands, 2009; pp. 117–139.
10. Khiabani, Y.S.; Wei, S.; Yuan, J.; Wang, J. Enhancement of secrecy of block ciphered systems by deliberate noise. *IEEE Trans. Inf. Forensics Secur.* **2012**, *7*, 1604–1613. [CrossRef]
11. Wei, S.; Wang, J.; Yin, R.; Yuan, J. Trade-off between security and performance in block ciphered systems with erroneous ciphertexts. *IEEE Trans. Inf. Forensics Secur.* **2013**, *8*, 636–645. [CrossRef]
12. Oggier, F.; Mihaljević, M.J. An information-theoretic security evaluation of a sass of randomized encryption schemes. *IEEE Trans. Inf. Forensics Secur.* **2014**, *9*, 158–168. [CrossRef]
13. Mihaljević, M.J.; Oggier, F. Security evaluation and design elements for a class of randomized encryptions. *IET Inf. Secur.* **2019**, *13*, 36–47. [CrossRef]
14. Kavčić, A.; Mihaljević, M.J.; Matsuura, K. Light-weight secrecy system using channels with insertion errors: Cryptographic implications. In *Proceedings of IEEE Information Theory Workshop (ITW) 2015*; IEEE Press: Piscataway, NJ, USA, 2015; pp. 257–261.
15. Mihaljević, M.J.; Kavcić A.; Matsuura, K. An encryption technique for provably secure transmission from a high performance computing entity to a tiny one. *Math. Probl. Eng.* **2016**, *2016*. [CrossRef]
16. Coppersmith, D.; Krawczyk, H.; Mansour, Y. The shrinking generator. (CRYPTO '93). *Lect. Notes Comput. Sci.* **1994**, *773*, 22–39.
17. Meier, W.; Staffelbach, O. The self-shrinking generator, (EUROCRYPT'94). *Lect. Notes Comput. Sci.* **1995**, *950*, 205–214.
18. Mihaljević, M.J. A faster cryptanalysis of the self-shrinking generator. (ACISP 1996). *Lect. Notes Comput. Sci.* **1996**, *1172*, 182–189.
19. Hell, M.; Johansson, T. Two New Attacks on the Self-Shrinking Generator. *IEEE Trans. Inf. Theory* **1994**, *52*, 3837–3843. [CrossRef]
20. Cardell, S.D.; Fuster-Sabater, A. *Cryptography with Shrinking Generators*; Springer Briefs in Mathematics; Springer: Cham, Switzerland, 2019.
21. Thomas, E.K.; Tan, V.Y.F.; Vardy, A.; Motani, M. Polar coding for the binary erasure channel with deletions. *IEEE Commun. Lett.* **2017**, *21*, 710–713. [CrossRef]
22. Tebbe, D.L.; Dwyer, S.J., III. Uncertainty and the probability of error. *IEEE Trans. Inf. Theory* **1968**, *IT-24*, 516–518. [CrossRef]
23. Feder, M.; Merhav, N. Relations between entropy and error probability. *IEEE Trans. Inf. Theory* **1994**, *40*, 259–266. [CrossRef]
24. Cheraghchi, M. Capacity upper bounds for deletion-type channels. *J. ACM* **2019**, *66*, 9. [CrossRef]
25. Katz, J.; Lindell Y. *Introduction to Modern Cryptography*; CRC Press: Boca Raton, FL, USA, 2007.